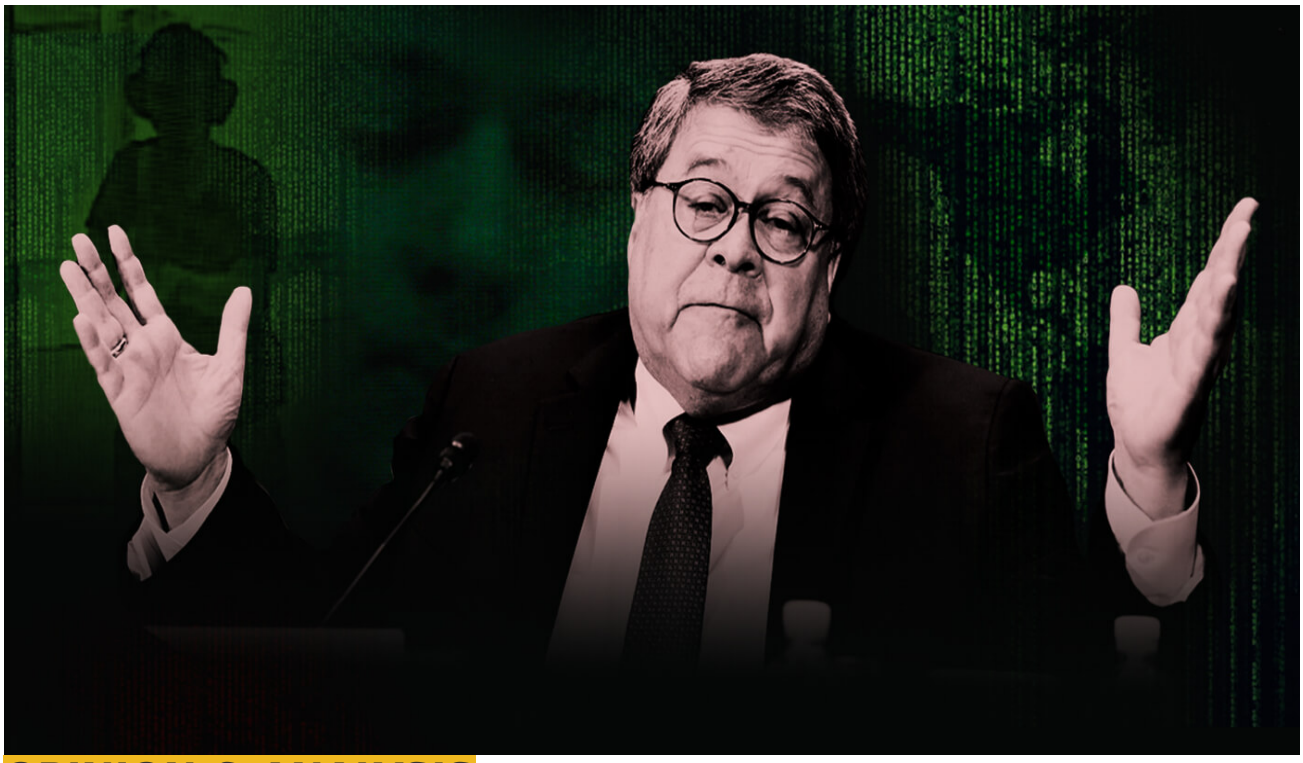


OPINION & ANALYSIS

DidDid Bill Barr Call His Shot? Unanswered Questions about FBI's Foreknowledge of the El Paso Shooting

by *Whitney Webb*

By **Whitney Webb**

0 Comments

As a series of recent mass shootings have brought renewed demands for the U.S. government to do something to address the spike in "lone wolf" violence, the Trump administration's decision to blame internet privacy, controversial websites like 8chan, and social media for the shootings has raised eyebrows from across

the political spectrum, particularly in light of claims that Trump's recent rhetoric about immigrants may have incited some of the shooters.

During a press conference on Monday, Trump blamed the internet for the three most recent mass shooting events:

> *We must recognize that the internet has provided a dangerous avenue to radicalize disturbed minds and perform demented acts. We must shine light on the dark recesses of the internet and stop mass murders before they start.... The perils of the internet and social media cannot be ignored, and they will not be ignored... We cannot allow ourselves to feel powerless. We can and will stop this evil contagion."*

Yet, not long before the recent spate of mass shootings began, U.S. Attorney General William Barr gave a speech on July 23 in which he spoke of the need for all consumer electronic devices and encrypted software to have a backdoor for the government to bypass encryption, essentially calling for many of the same measures that Trump has proposed *following* the recent shootings.

Notably, Barr concluded his speech by stating that he anticipated "a major incident may well occur at any time that will galvanize public opinion on these issues." In other words, just a few days prior to the recent spate of mass shootings, William Barr stated that he anticipated a public safety crisis that "may well occur at any time" and would reduce public resistance to the further erosion of civil liberties that he was advocating for in his speech.

Furthermore, the FBI, which operates under the jurisdiction of the Department of Justice and reports directly to William Barr, has now stated that it was aware of the El Paso shooter's plan to

murder civilians via a post made on 8chan at least two hours before the shooting took place. 8chan — a controversial website that the FBI is known to have used to incite violence as part of its controversial terrorist entrapment strategy — has since been banned in the shooting's aftermath. In addition, less than two months ago, the FBI obtained a warrant for 8chan's host — Ch.net — in which the Bureau demanded access to the entire contents of the accounts that were of interest in that specific investigation, suggesting that the FBI had increased access to information of hundreds of 8chan accounts in the lead-up to the recent shootings.

The overlap between Barr's recent speech and Trump's proposed solution to the massacres, as well as the FBI's unusual recent relationship with 8chan, has led some to suggest that the Trump administration is taking advantage of the tragedy at El Paso and of other recent mass shootings to impose unpopular restrictions on civil liberties and increase the mass surveillance of innocent Americans.

An uncanny prediction

On Tuesday, July 23, Attorney General William Barr gave the keynote address at the 2019 International Conference on Cyber Security (ICCS) at Fordham University. The focus of Barr's speech was the need for consumer electronic products and applications that use encryption to offer a "backdoor" for the government, specifically law enforcement, to obtain access to encrypted communications as a matter of public safety.

Early in his speech, Barr stated:

> *Service providers, device manufacturers and application developers are developing and deploying encryption that can only be*

> *decrypted by the end user or customer, and they are refusing to provide technology that allows for lawful access by law enforcement agencies in appropriate circumstances.…*
>
> *While encryption protects against cyberattacks, deploying it in warrant-proof form jeopardizes public safety more generally. The net effect is to reduce the overall security of society.”*

Barr went onto say that “warrant-proof encryption is also seriously impairing our ability to monitor and combat domestic and foreign terrorists.” Barr stated that “smaller terrorist groups and ‘lone wolf’ actors” — such as those involved in the series of mass shootings in California, Texas and Ohio that would occur in the weeks after his speech — “have turned increasingly to encryption.” Barr later notes that he is specifically referencing encryption used by “consumer products and services such as messaging, smart phones, email, and voice and data applications.”

Barr then laid out his vision of what the solution to this challenge posed by “warrant-proof encryption” would look like:

> *We believe that when technology providers deploy encryption in their products, services, and platforms they need to maintain an appropriate mechanism for lawful access. This means a way for government entities, when they have appropriate legal authority, to access data securely, promptly, and in an intelligible format, whether it is stored on a device or in transmission.*
>
> *We do not seek to prescribe any particular solution. Our private-sector technology providers have immensely talented engineers who have built the very products and services that we are talking about. They are in the best*

> *position to determine what methods of lawful access work best for their technology."*

After laying out his vision, Barr stated that, while he would like to give private companies time to willingly cooperate and comply with his suggested solution to "warrant-proof encryption," "the time to achieve that [government back-doors into electronic consumer apps and products] may be limited."

To overcome the resistance by some private companies — who do not want to renege on their right to privacy by giving the government back-door access to their devices — and American consumers, Barr tellingly anticipates that a "major incident" will soon take place that will mold public opinion in favor of his proposed solution.

Barr concluded his speech by stating:

> *I think it is prudent to anticipate that **a major incident** may well occur at any time that **will galvanize public opinion on these issues**.*
>
> *As this debate has dragged on, and deployment of warrant-proof encryption has accelerated, our ability to protect the public from criminal threats is rapidly deteriorating. The status quo is exceptionally dangerous, unacceptable, and only getting worse.*
>
> *The rest of the world has woken up to this threat. It is time for the United States to stop debating **whether** to address it, and start talking about **how** to address it." (emphases added)*

On Thursday, July 25, the last day of the ICCS conference, FBI Director Christopher Wray also echoed Barr's call for government

back-doors into encrypted software and apps, stating in his speech:

> *Cybersecurity is a central part of the FBI's mission. But as the attorney general discussed earlier this week, our request for lawful access cannot be considered in a vacuum. It's got to be viewed more broadly, taking into account the American public's interest in the security and safety of our society, and our way of life. That's important because this is an issue that's getting worse and worse all the time.*
>
> *There's one thing I know for sure: It cannot be a sustainable end state for us to be creating an unfettered space that's beyond lawful access for terrorists, hackers and child predators to hide. But that's the path we're on now, if we don't come together to solve this problem."*

A new phase of an old campaign

The speeches given by Barr and Wray are the most recent iterations of the Department of Justice's years-long effort to evade and weaken the encryption used by certain electronic products and applications, particularly encrypted messaging apps. Indeed, the DOJ was particularly active in late 2017 in pushing for back-doors into encrypted software, citing the encrypted devices of past perpetrators of mass shootings as proving the need for federal law enforcement to easily and quickly bypass encryption in criminal investigations.

However, Barr's and Wray's speeches mark a new phase of this government campaign targeting encryption, a campaign that has picked up in the past two weeks just as a series of mass

shootings in the United States have led to widespread calls for the government to do something to prevent further massacres.

At a Monday press conference, President Donald Trump gave his official response to the most recent shootings in Ohio and Texas, tragedies that he largely blamed on the internet and its “dark recesses” that are inaccessible to the government. “We must recognize that the internet has provided a dangerous avenue to radicalize disturbed minds and perform demented acts,” Trump stated, before adding: “We must shine light on the dark recesses of the internet and stop mass murders before they start.”

“The perils of the internet and social media cannot be ignored and they will not be ignored,” the president emphasized.

One of the main solutions Trump offered to what he alleged caused the recent shootings was to mandate the DOJ “to work in partnership with local, state and federal agencies as well as social media companies to develop tools that can detect mass shooters before they strike.” Some interpreted this statement as suggesting the more widespread implementation of “pre-crime” software, such as Palantir, which was co-founded by billionaire Trump backer Peter Thiel, who is also on Facebook’s board.

Conveniently for William Barr, Facebook announced in May that the company is already developing just the “backdoor” that the attorney general has sought. This new initiative would implement AI-powered surveillance measures onto consumer devices, which would bypass end-to-end encryption on both the recently encrypted Facebook Messenger and the popular encrypted messaging app WhatsApp, acquired by Facebook in 2014. Though the measure was announced in May, it has received media attention only in the last week, following Barr’s speech at the 2019 ICCS.

Following Trump's proposal for social media and the Barr-led DOJ to work together to monitor encrypted messages, it seems that Facebook will be one of the first major tech companies to offer its ready-made solution to the U.S. government. It is also worth considering the possibility that Barr may use the threat of his Silicon Valley antitrust probe to potentially strong-arm tech companies that would otherwise be unwilling to create a government back-door in their software or products. That probe was announced the same day that Barr spoke about anti-encryption measures at the 2019 ICCS.

In addition, between Barr's July 23 speech and Trump's August 5 press conference, there has been a concerted push from not only the DOJ but also the Five Eyes intelligence alliance, of which the U.S. is part, to weaken encryption or give governments access to encrypted applications.

On the heels of the 2019 ICCS, at which Barr and Wray spoke, there was a related cyber security summit in London — called the Five Country Ministerial — where "senior ministers from the U.K., Australia, Canada, New Zealand and the United States … reaffirmed their commitment to work together with industry to tackle a range of security threats."

According to the U.K. government's press release on the summit, which took place from July 29 to 30, the ministers in attendance "stressed that law enforcement agencies' efforts to investigate and prosecute the most serious crimes would be hampered if the industry carries out plans to implement end-to-end encryption, without the necessary safeguards." William Barr attended that summit, representing the U.S., and echoed his speech given a week prior, stating:

> *We must ensure that we do not stand by as advances in technology create spaces where criminal activity of the most heinous kind can go undetected and unpunished."*

Notably, Australia last year implemented a law similar to that which Barr is seeking to enact in the United States. It has since been lampooned by expert cryptographers for its ineffectiveness and has caused damage to Australia's tech industry. According to the *Guardian*, Microsoft revealed in March that companies and governments it works with say they "are no longer comfortable about storing their data in Australia as a result of the encryption legislation." Perhaps predictably, what has happened since Australia's enactment of this controversial encryption legislation is the Australian government's use of its new "back-doors" to widely surveil its civilians without a warrant.

Barr's Orwellian bent

Barr's outsized involvement in this recent push for a government back-door into all encryption apps is notable given his past. For instance, prior to becoming attorney general under Trump, Barr worked at the law firm Kirkland & Ellis, a firm that "represent[s] clients on matters relating to data and network security." Kirkland & Ellis, in describing its own services, notes:

> *These matters are increasingly important to national security and international trade concerns such as government surveillance issues, state-sponsored cyber-attacks and espionage, and legal limitations on cross-border data transfers. The Firm represents clients in navigating these legal matters, including with respect to investigating security incidents/breaches and handling resulting litigation or government relations aspects of such incidents."*

Furthermore, Barr's previous stint as attorney general, during the administration of George H.W. Bush, saw him push for increasing mass surveillance of innocent Americans. According to *USA*

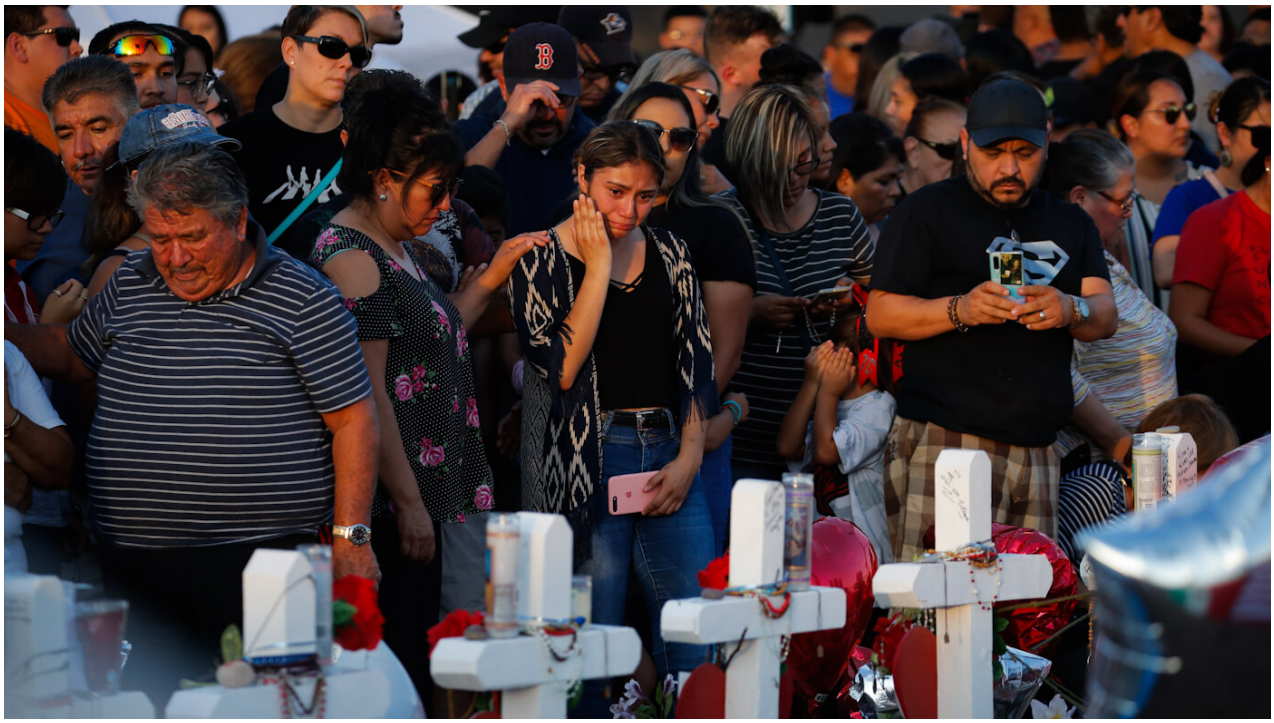
Today, in 1992, while serving as Attorney General under Bush Sr., Barr “launched a vast surveillance program that gathered records of innocent Americans’ international phone calls without first conducting a review of whether it was legal.” The program “ultimately gathered billions of records of nearly all phone calls from the United States to 116 countries, with little oversight from Congress or the courts” and also “provided a blueprint for far broader phone-data surveillance the government launched after the terrorist attacks of Sept. 11, 2001.” The program was partially carried out by the then-head of the DOJ’s Criminal Division, former FBI Director Robert Mueller.

Barr’s history of pushing for reducing privacy for citizens is troubling considering that, earlier in his career, he pushed for increased government secrecy while he was employed by the CIA in the late 1970s. For instance, while working at the CIA’s Office of Legislative Council, Barr attempted to circumvent the moratorium placed on the CIA that prevented it from destroying records and also stonewalled the Church Committee’s investigation into CIA abuses. Thus, Barr’s push for reduced privacy for citizens but increased privacy for the government bodes poorly for those who see government transparency and citizen privacy as important to keeping government overreach in check.

FBI foreknowledge

In the hours before the shooting at a Walmart in El Paso, Texas — and less than two weeks after Barr warned of an imminent “major incident” that would “galvanize public opinion” in favor of ending encryption free from a government back-door — the FBI was made aware of a manifesto published on the controversial website 8chan that is alleged to have been authored by the shooter, Patrick Crusius.

According to *NBC News*, the FBI was aware of the document prior to the shooting, but was unable to act quickly enough to prevent the attack. There have, however, been conflicting reports about exactly how long the FBI was aware of the alleged manifesto prior to the shooting.



People visit a makeshift memorial at the scene of a mass shooting at a shopping complex, Aug. 6, 2019, in El Paso, Texas. John Locher | AP

For instance, soon after the shooting, *CNN* stated that three different sources had told the outlet that the manifesto had been "posted days before the shootings." However, the FBI later stated less than a half hour before the shooting, while separate law enforcement sources told reporters that it was actually two hours before the shooting.

There is also a discrepancy regarding whether the manifesto was originally posted on 8chan and whether the shooter himself even posted it. Jim Watkins, who owns the 8chan message boards and has alerted federal authorities previously when past shooting manifestos were published at the site, stated:

> *First of all, the El Paso shooter posted on Instagram, not 8chan…Later, someone uploaded the manifesto. However, that manifesto was not uploaded by the Walmart shooter. I don't know if he wrote it or not, but it was not uploaded by the murderer; that is clear."*

Facebook, which owns Instagram, said that it had disabled an Instagram account that belonged to Crusius and also noted that that account had been inactive for over a year.

In the past, 8chan administrators had deleted manifestos minutes after they were posted and warned federal authorities that the documents had been published. In the case of the El Paso shooting, Watkins claimed that the site had informed federal authorities as soon as they were aware that the manifesto had been uploaded to its page.

The facts that the FBI knew in advance of the manifesto, that the manifesto may not have been uploaded by the shooter, and that the FBI was quick to link that document to the shooting event soon after it took place have led to speculation about how the FBI was able to make that connection so quickly. For instance, lawyer Robert Barnes stated the following on Twitter:

> *How did [the] FBI identify the shooter before he began his attack from a post on an anonymous chat board? Usually, this means the shooter tipped them off either directly or indirectly (informant). Misuse of informants (including encouraging violence) is an underexplored problem."*

In addition, journalist Rachel Blevins posed a similar question on social media following the revelations, writing:

> *It took just hours for the FBI to both identify the suspect in the El Paso shooting and connect him to a manifesto posted on 8chan, which raises the question… was the suspect included in the FBI's surveillance, and were their agents in contact with him before the shooting?"*

This possibility is worth considering, given the well-documented history of the FBI's policy of manufacturing domestic terror plots within the United States, most of which are ultimately foiled at the last minute by the Bureau. In many of those cases, many alleged terrorists would not have planned or attempted those attacks without goading and support from the FBI, leading critics to accuse the FBI of deliberately using entrapment. For instance, a 2014 study by Human Rights Watch and Columbia Law School's Human Rights Institute found that "many of these people [in the cases examined in the study] would never have committed a crime if not for law enforcement encouraging, pressuring, and sometimes paying them to commit terrorist acts," according to the study's co-author Andrea Prasow.

There are several instances where the FBI sought out mentally handicapped and unstableindividuals with no resources of their own, giving them incentives, fake weapons and even driving them to the scene of the planned terror attack. Two high-profile domestic terror cases have also had hints of FBI involvement — including the Pulse nightclub shooting, where the shooter's father was later revealed to be an FBI informant and the FBI had attempted to goad the Pulse shooter into committing a terror attack years prior to the Pulse shooting. In addition, the family of the Boston Marathon bombers claimed that the FBI regularly visited their family home and had cultivated a relationship with one of the bombers, Tamerlan Tsarnaev, prior to the bombing.

Since late 2016, the FBI's controversial policy of inducing individuals to commit acts of terror in the United States has expanded after a federal appeals court ruling in December of that year said that federal agents were allowed to target and

manipulate a person's religious beliefs and entrap them in terror act schemes as a way to "probe the attitudes" of that targeted individual. The ruling also permitted federal agents to create false friendships, referred to in the ruling as the "illusory cultivation of emotional intimacy," as a means of manipulating individuals to commit acts of terrorism — as well as providing these unstable individuals with money, vehicles, businesses and even vacations to get them to agree to participate in attacks. All the FBI needs to prove in return is that the entrapped individual, prior to being contacted by the FBI, was "predisposed" to commit a crime.

As a result of this troubling trend, and given the FBI's foreknowledge of the manifesto and its ease in connecting that document to the shooter, it becomes important to ask whether the FBI had more foreknowledge of the situation than it has publicly let on.

Though history indicates that FBI foreknowledge of the shooter is definitely plausible, 8chan has been a recent focus of the FBI in recent months. For instance, after the alleged manifesto of the shooter responsible for the massacre at the Poway Synagogue earlier this year was published on 8chan, the FBI issued a warrant for hundreds of 8chan user accounts that had commented on the Poway Synagogue shooter's thread, including both users that supported his statement of intent and those who were appalled by it.

According to the Bureau's application for a search warrant, the FBI was seeking the "IP address and metadata information about [Poway shooter John] Earnest's original posting and the postings of all of the individuals who responded to the subject posting and/or commented about it." The FBI further instructed Ch.net, which hosts 8chan, "to make a digital copy of the entire contents of the accounts subject to seizure."

Download the PDF file .

It goes without saying that with the information on hundreds of 8chan users, the FBI would have had access to potential future informants and potential targets to be “groomed” by the FBI for a future domestic terrorism entrapment case. This is especially likely given that the FBI’s reasoning for obtaining this large amount of information in the warrant was to identify “individuals who are inspired by the subject posting [i.e., the Poway shooter manifesto].” One 8chan user who was contacted by the FBI after this search warrant and filmed the encounter, was asked by federal agents to help them with information-gathering on other 8chan users.

This possibility is further supported by the fact that the FBI agent who filed the search warrant application, FBI Special Agent Michael Rod, revealed that he had been active on 8chan and (perhaps inadvertently) revealed his user name on 8chan to be user “8f4812.” An archive of the Poway shooter’s 8chan thread, available here, reveals that Rod stated in that 8chan thread that Russia was to blame for the Poway shooting and Rod also claimed that he knew of the Poway shooting 15 minutes before it happened but was unable to warn the authorities because he “was shit posting and got tied up.”

In the wake of the recent shootings in El Paso, Texas and Dayton, Ohio, 8chan was taken offline after internet infrastructure company Cloudflare declined to continue supporting the website.

A tragedy foretold and exploited

William Barr’s warning that a “major incident” could occur “at any time” and “galvanize public opinion” around the unpopular encryption back-door policy he has been seeking seems to have come true in the weeks since the attorney general made those statements. Given Barr’s influence over the FBI, which operates under his jurisdiction, it is important to scrutinize the evidence

that the FBI had apparent foreknowledge of at least one of these recent shootings, and consider that the Bureau may have failed to act to prevent the tragedy, allowing Barr's prediction just weeks earlier to become a self-fulfilling prophecy.

Trump's proposed solution to the recent spate of mass shootings is focused on giving Barr a mandate to work with social media and tech companies to prevent another mass shooting before it occurs. It seems evident that this solution is set to involve surveilling encrypted communications to ostensibly prevent another shooting while also providing Barr, and the DOJ at large, the back-door into encrypted apps and consumer products that they have long sought but have been unable to sell to either the public or those same tech companies.

Now, a public safety crisis has emerged in the wake of Barr's recent speech, tipping the scales — as Barr had predicted — so the public would favor further reductions to their civil liberties and right to privacy so that the federal government could provide increased public safety through increased surveillance. Yet, taking this alongside the well-documented fact that the FBI regularly manufactures domestic terror plots, it is worth asking whether some of these recent shootings were allowed to happen and whether public officials like William Barr are manipulating the public's reaction to these tragedies to advance their own political agendas and further the build-up of state power.

Feature photo | Graphic by Claudio Cabrera

Whitney Webb *is a MintPress News journalist based in Chile. She has contributed to several independent media outlets including Global Research, EcoWatch, the Ron Paul Institute and 21st Century Wire, among others. She has made several radio and television appearances and is the 2019 winner of the Serena Shim Award for Uncompromised Integrity in Journalism.*

The views expressed in this article are the author's own and do not necessarily reflect MintPress News editorial policy.

0 Comments

- 8CHAN
- EL PASO
- ENCRYPTION
- MASS SHOOTINGS
- PUBLIC OPINION
- WILLIAM BARR